

APPENDIX B

Best Practices for Government Use of CCTV: Implementing the Fair Information Practice Principles

Introduction

The Department of Homeland Security (DHS) Privacy Office and Office for Civil Rights and Civil Liberties are issuing *Best Practices for Government Use of CCTV: Implementing the Fair Information Practice Principles* to educate government agencies interested in building privacy, civil rights, and civil liberties considerations into Closed Circuit Television (CCTV) system design, acquisition, and operations. Government agencies are encouraged to use these best practices to build and operate CCTV systems that improve law enforcement effectiveness while preserving privacy and civil liberties. Taking such actions now can help ensure that efforts to improve security do not lead to the creation of a surveillance society.

In addition to considering implementation of these best practices, law enforcement leaders and political decision makers should carefully consider conducting a cost-benefit analysis before selecting CCTV over other tools to fight crime or improve security. A CCTV program is more likely to gather public support when the protected community understands the objectives of the program and knows that it is the result of a thoughtful analysis.

These best practices are written using the widely-accepted framework known as the Fair Information Practice Principles (FIPPs). These principles are: Transparency, Individual Participation, Purpose Specification, Data Minimization, Use Limitation, Data Quality and Integrity, Security, and Accountability and Auditing. The eight FIPPs are at the core of the Privacy Act of 1974 [5 U.S.C. § 552a] and are mirrored in the laws of many U.S. states as well as many foreign nations.

Material for drafting these best practices was also drawn from the proceedings of the DHS Privacy Office Public Workshop, *CCTV Developing Privacy Best Practices*, which was held on December 17 -18, 2007, and the comments filed in conjunction with the workshop. At that workshop, elected U.S. and international officials, law enforcement executives, public interest advocates, academics, and technologists offered a variety of opinions on best practices for implementing CCTV systems while respecting privacy and civil liberties. The discussion of best practices focused on practical recommendations for law enforcement agencies. A report of the highlights of the workshop, along with a complete transcript and comments filed, are available at www.dhs.gov/privacy.

The DHS Privacy Office and the Office for Civil Rights and Civil Liberties are undertaking the development of these best practices to fulfill their statutory duties, and the Department's mission to protect the homeland, including preserving our freedoms and our way of life. Section 222 (a)(2) of the Homeland Security Act of 2002, as amended [6 U.S.C. 552142], as amended, directs the Chief Privacy Officer of DHS to assure that the Fair Information Practice principles are implemented at the Department. The DHS Officer for Civil Rights and Civil Liberties is

directed in Section 705 (a)(3) of the Act, as amended [6 U.S.C. § 345] to “ensure that the protection of civil rights and civil liberties is appropriately incorporated into Department programs and activities.” Because the Department funds the purchase of CCTV systems and analogous technology through Homeland Security Grants and other programs, DHS Privacy Office and the Office for Civil Rights and Civil Liberties believe it is important for DHS to help inform government agencies on how to implement CCTV programs in a manner that respects these fundamental rights and values.

These best practices do not take a position on the costs or benefits of CCTV, but rather provides a list of considerations a government agency should address as part of its decision making and planning. The DHS Privacy Office and the Office for Civil Rights and Civil Liberties invite the public to comment on these best practices, as they may be revised in the future as the technology evolves, and based on experience gained from its implementation and from public comments. Comments or questions regarding these best practices may be sent to privacy@dhs.gov.

Fair Information Practice Principles (FIPPs)

The privacy principles outlined here are based upon the FIPPs, a set of principles that have long served as a framework for protecting privacy within the United States and internationally. These principles were first articulated in the U.S. Department of Health, Education, and Welfare’s 1973 report entitled, *Records, Computer, and the Rights of Citizens: Report of the Secretary’s Advisory Committee on Automated Personal Data Systems*. The report identified eight practices, which later served as a basis for the U.S. Privacy Act of 1974.

The U.S. government has also long promoted the FIPPs internationally. In 1980, the FIPPs served as the basis for the 1980 Organization for Economic Cooperation and Development (OECD) *Guidelines on the Protection of Privacy and Transborder Flow of Personal Data*. Later in 1995, a variation of these principles was the basis of the European Union Data Protection Directive. As recently as 2004, the FIPPs were championed again by the United States in the development of the Asia-Pacific Economic Cooperation (APEC) Privacy Framework.

Section 222 of the Homeland Security Act of 2002, as amended, which is the basis for the authorities and responsibilities of the DHS Chief Privacy Officer, also recognizes the significance of the FIPPs, calling on the Chief Privacy Officer to “assur[e] that personal information contained in Privacy Act systems of records is handled in full compliance with *fair information practices* as set out in the Privacy Act of 1974.” (Italics added for emphasis.) Pursuant to Section 222, the Privacy Office has applies the FIPPs in its Privacy Impact Assessment guidance and throughout its operations.

The best practices articulated below apply these widely-held principles to the privacy concerns associated with the government’s use of CCTV. Each FIPPs principle is followed by examples of how to implement the principle in the context of CCTV.

Purpose Specification Principle

Each government agency should specifically articulate the authority that permits its use of CCTV and specifically articulate the law enforcement purpose(s) for which CCTV is intended to be used.

- (1) Know why you want to deploy CCTV. What is your current law enforcement strategy and what role can CCTV play?
 - a) To the extent feasible, conduct a study or literature review of the effectiveness of CCTV for the intended purpose. Consideration of how CCTV might be employed effectively (or how it might not be helpful) may assist in the decision making. Make the results of the study available to the public.
 - b) Determine whether CCTV is intended to assist in for crime detection, crime prevention, or to assist in crime investigations, or to secure critical infrastructure from possible terrorist threat.
 - c)
 - d) Evaluate whether there are alternative means of addressing the stated purpose, particularly alternatives that are less intrusive on privacy and civil liberties. Alternatives may include area lighting, community policing, or crime prevention programs to address root causes.
 - e) Determine whether resources will be available, long term, to properly operate the system properly. This should take into account funding, staffing, physical logistics, and maintenance, among other things.
- (2) Know whether you have the legal authority to employ CCTV.
 - a) Have a clearly articulated law enforcement purpose before setting up a CCTV system. Continue to ask when designing, building, and operating the system, whether it is capable of effectively achieving that purpose.

Example: Determine whether the system will serve a crime prevention or evidentiary purpose and develop appropriate protocols for such purpose(s).
- (3) The cameras and the camera network should be equipped with only those features or capabilities reasonably necessary to serve the purpose of the system. Technological features like magnification, night vision, infrared detection, and automatic identification and tracking, which pose significant dangers to privacy and other constitutional rights and liberties, should be used only where they are needed.
 - a) Example: A camera network created to monitor a busy urban freeway for accidents or stopped vehicles likely does not require facial recognition technology—the use of which would increase the impact on civil liberties and increase the cost of the system without furthering its legitimate purpose.

Transparency Principle

Each government agency considering the use of CCTV should be as transparent as possible and provide notice to the public regarding its use of CCTV. There should be no secret use of CCTV. Each agency should have a written CCTV policy that governs the collection, use, maintenance, and disclosure of all camera footage or images.

- (1) Where possible, involve the community in the decision making process to adopt CCTV.
Establishing surveillance within a community can have major impact because even ordinary, law-abiding people may resent the presence of an “all-seeing eye.”
 - a) Government agencies should give community stakeholders adequate notice when considering the use of CCTV and provide an opportunity for meaningful public comment. In addition to gauging possible community response to an installed CCTV system, this presents the decision-makers with a chance to win community support, which can contribute to the success of law enforcement and security efforts in the future.
 - b) The process should be public and include public notice, an assessment of how the system will likely impact privacy and civil liberties, and should state how the system will be authorized. A CCTV initiative will be better received if it is the subject of deliberations and is rolled out with the assent of politically accountable officials, such as city council members or an elected law enforcement officer.
 - c) Town meetings, deliberation by the elected governance of a city or town, administrative notice and comment process, public hearings, voter referendum or neighborhood canvassing are all acceptable means of involving the public and demonstrating government accountability.
 - i) Stakeholders include representatives from law enforcement, homeland security, emergency management, academic, legal, political, business, civic, religious, civil liberties protection, and technologists, as well as those citizens who wish to participate in the public process.
- (2) Conduct a cost-benefit analysis as part of the decision making process and make that information available to the public.
 - a) Conducting such an analysis may be difficult given that privacy and civil liberties are difficult to quantify; however, a number of factors can be evaluated: locations, number of cameras, capabilities, type of network, database design, storage retention, active or inactive monitoring, security measures, and alternatives.
- (3) Prepare a written policy defining the mission of the system, how the cameras will be used, the rules of operation, and the privacy and civil liberties protections that have been provided to protect against misuse or abuse.
 - a) Identify the system administrator responsible for all operational and administrative elements.
 - b) Explain the system’s capabilities; how it will be used, image retention, and release; and access to video center and image storage locations.
 - c) Note the legal and administrative restrictions for its use.
 - i) Address the privacy and civil liberties concerns discussed in this guidance.
 - ii) Consider issues such as maintaining the integrity of evidence, the possible uses of CCTV footage and images (prosecution, defending against or substantiating officer abuse claims) as well as more troublesome uses (*e.g.*, subpoena by third parties attempting to prove or disprove matters at issue in unrelated civil litigation, such as divorce cases).
- (4) Make as much of the agency’s documentation (*e.g.*, policy, standard operating procedures, records disposition schedule, etc.) as possible publicly available.

Individual Participation Principle

Each government agency considering the use of CCTV should involve the public to the greatest extent possible in its decision to employ CCTV. Ideally, public involvement should take place before the agency applies for grant funding from the Department of Homeland Security. To the extent practical, the agency should provide notice through appropriate signage in areas where CCTV is employed and provide mechanisms for appropriate access and redress regarding the use of camera footage or images.

- (1) Provide individuals a method to access images of themselves, if the camera footage or images are retained in a manner that identifies the individual and permits retrieval.
- (2) Access rights, however, should not be used to justify archiving footage.
- (3) Time-limited archiving is always preferable from a privacy perspective and possibly from a system management standpoint as well.
 - a) Data retention and storage quickly becomes very expensive, and the stored data is frequently useless.
 - b) A short retention period will reduce the number of access requests.
 - c) A well-designed policy for a system that stores data should include procedures for identifying footage or images that should be retained, indexing and storing it in a retrievable manner, and establishing a chain of custody over footage or images that may be of legal significance.
- (4) A policy that some CCTV system operators have found useful in this respect is permitting individuals to inspect, at any reasonable time (*e.g.*, in a non-crisis period and without compromising the security of critical infrastructure), the agency's camera monitoring operations center. In addition to permitting individual access and establishing transparency and oversight, this can serve an important public relations purpose, reassuring the community about the reasonableness of the CCTV use and the good faith of the CCTV operators. Agencies permitting this type of open access to CCTV operations report community support for monitoring.

Data Minimization Principle

Each government agency should only use CCTV to the extent relevant and necessary to accomplish the specified purpose(s) and only retain the camera footage or images for as long as is necessary to fulfill the specified purpose(s). The camera footage or images should be disposed of in accordance with a specified records disposition schedule.

- (1) Design the scope and capabilities of the system to minimize its negative impact on privacy and other constitutional rights and values by limiting the data collected to the data that is likely to help accomplish the mission and limiting the data retained to the data that is necessary to accomplish the mission.
 - a) Data minimization aligns with many pragmatic concerns.
 - i) Excess surveillance capacity does not produce good value-for-money due to the cost of standing up and operating systems, and the cost of data storage.

- ii) Excess surveillance capacity may increase the chance of improper activity by system operators. More cameras and more operators mean more chances for all types of complications.
 - iii) Given the bandwidth of video feeds, long term data storage can be costly, especially when useless data is retained.
- (2) Data collection should be time, geographically, and technically limited to accomplish only the system's stated goals.
 - a) The duration that a system operates should be no longer than reasonably necessary to achieve its articulated purpose.
 - i) Permanent systems should be created only to address threats to public safety that are of indefinite duration.
 - (1) Example: CCTV system monitoring vulnerable approaches to a liquid propane gas terminal.
 - ii) Agencies should evaluate camera systems annually (including efficacy studies), and determine if they are still necessary.
 - iii) Flexible installation of cameras, permitting ready removal and reinstallation elsewhere as required, may be a cost effective way of achieving law enforcement and security goals, while limiting the amount of irrelevant data collected.
 - iv) Data retention and disposal policies should be decided ahead of time.
 - (1) Images and footage should not be permanently retained, unless there is a purpose to the retention, such as use in an ongoing investigation of specific persons or activities, or availability for court testimony in a proceeding.
 - (2) Retained data can be subpoenaed by outside civil litigators, for example, in divorce cases.
 - (3) Communities might not be receptive to CCTV programs that create a permanent record of the activities of innocent people in areas under surveillance.
 - (4) Data retention can still be expensive, even though costs are going down.
 - b) CCTV systems should be limited in geographic scope, serving as extra eyes in problem areas (*e.g.*, with law enforcement or security problems) and looking only at areas where it is permissible and non-oppressive for law enforcement officers and security personnel to look.
 - i) Thus far, studies indicate that CCTV systems work best when targeting specific areas that have specific problems. Cameras may create a "squish zone," moving crime off one street and into an alley, or onto the next street. Coupled with other law enforcement strategies, this may be useful. In contrast, surveilling an area of little law enforcement or security concern is without purpose, resulting in the accumulation of useless data and the unnecessary expenditure of funds.
 - ii) Use only enough cameras to accomplish the intended purpose.
 - iii) Only focus cameras on those structures or areas that require law enforcement or security scrutiny, and where observation will fit into the overall law enforcement or security strategy.
 - (1) Example: Surveillance of a public park may be a reasonable use, but the cameras overlooking the park should not also be able to look into the windows of an adjacent apartment building.
 - (2) Example: An optical camera with very high magnification provides generally observation capability in observes a public square, but it may also be capable of

reading what an individual at an outdoor café table some distance away is writing on a note pad.

- c) CCTV systems should be limited in the types of technology employed to those types of technology necessary to accomplish the goals of the system.
 - i) Example: A traffic monitoring CCTV system should probably not be designed with facial recognition analysis in mind.
 - ii) Example: A camera in a public space combined with audio feed for detecting gunshots should not be used to eavesdrop on conversations of passersby.
 - iii) Example: If simple, visual observation of a public area like a plaza is the goal, the system should not include technology to capture and record conversations of individuals within the vicinity.
 - iv) Example: Consider whether cameras should be fitted with technology that permits the ability to look through clothes or into containers in a public space.
 - v) Using sensors rather than cameras can limit the amount of data collected and the impact on privacy.
 - (1) Example: Law enforcement wants to partner with an oil refinery to secure a large, fairly desolate area around the plant. Instead of having dozens of cameras covering every approach at all time, several more powerful pan-tilt-zoom cameras are installed on elevated poles, which are automatically triggered to focus on a particular area when a motion sensor is triggered.
 - (2) Example: A large city has problems with gun violence. Rather than installing hundreds of cameras, sensitive audio sensors calibrated to detect gunshots can be installed to alert patrol units to the location of gunfire.
 - (3) Consider the privacy and civil liberties impact of installing audio sensors. Be sure that audio monitoring devices sensitive enough to detect gunshots at great distance are not used for eavesdropping.
 - d) To limit geographic and technical scope of CCTV systems, consider the following safeguards:
 - i) Fixed camera installation can prevent the camera from being re-targeted into private areas.
 - ii) Physical “blindings” can be installed to reduce the camera’s field of vision to prevent cameras from being panned, tilted, or zoomed into private areas that raise no law enforcement or security concern.
 - iii) Software “blur” spots can permit pan, tilt, and zoom operation, but render privacy areas too blurry for a viewer to interpret. Technical capability to unmask the blurring may be considered necessary to assist in a specific law enforcement investigation.
 - e) Consider emergency uses in CCTV design and build in enough flexibility to deal with such situations.
 - i) Example: A pan/tilt/zoom (PTZ) camera that routinely monitors a public square surrounded by housing may need to be refocused on private housing to follow an armed robber who has fled. Such cameras can be software limited to an ordinary sweep, but permit an operator to log in and view areas that would ordinarily not be examined. The log in would leave an audit trail, that would discourage impermissible uses and cause the operator to consider whether the planned camera use is permissible.
- (3) Legal considerations such as state privacy laws and the U.S. Constitution will also counsel data minimization.

- a) Example: Political demonstrators hold a peaceful demonstration in a public square observed by CCTV. The demonstration is uneventful. Whether it amounts to a violation of the First Amendment is unclear, but retaining footage or images of the event could have a chilling effect on the exercise of First Amendment rights, and should be avoided if possible. Such retention, as discussed above, may also be a waste of money and system resources.

Use Limitation Principle

Each government agency should use CCTV solely for the purpose(s) specified in the notice given to the public. Disclosing camera footage or images outside the agency should only be pursuant to a written policy and for a valid public safety or law enforcement purpose.

- (1) As a general matter, limit data sharing to those individuals and agencies with a legitimate need-to-know. More specifically, limit the number of individuals with access, the type and quantity of data shared, and the time that those individuals are permitted to retain the data.
- (2) Using camera footage or images for a purpose other than those stated in the public policy for the system, should only be done under special process to safeguard against abuse. Additional safeguards regarding secondary uses could include obtaining written authorization from a senior agency or law enforcement official or seeking permission from a local magistrate where constitutional or other individual rights questions arise.
 - a) Example: Assume a CCTV system includes audio monitoring for the purposes of gunshot detection, which passively monitors loud sounds and uses a vectoring process, similar to sonar, to determine where gunshots occurred. Generally, no monitoring of conversations or other noise by law enforcement occurs since the monitors are automated and tuned to detect gunshots. However, if law enforcement officers wish to eavesdrop on a meeting of two criminal conspirators scheduled for a public place under CCTV observation and request that the audio feed from the sensitive gunshot monitors be made available to them, state law may require the law enforcement officers to seek a warrant, and it may also be prudent under Federal Constitutional law to seek a warrant based on probable cause.
 - b) Example: Assume that a camera system with the stated purpose of monitoring a public plaza will sweep or be aimed toward a nearby park where a potentially violent political demonstration will occur. Because the use is planned and outside of the stated uses of the system, and additionally because significant individual rights issues are implicated, such use should require a senior law enforcement officer authorization.
 - c) No additional approval should be required for incidental use of a system.
 - i) Example: A system installed for crime control purposes should be available for use in assisting fire and rescue personnel in responding to a building fire or a plane crash. Similarly, exigent circumstances, such as monitoring fleeing suspects, should be permissible, subject to reasonable oversight measures.
 - ii) The types of incidental uses of the system that are permissible should be made clear to operators in training and in written policies.
 - iii) Data obtained during incidental/exigent use of the camera system should be reviewed by supervisors as soon as practical after the incidental use to determine if the data should be retained or purged.

- d) Secondary use of archived and “pre-archival” stored video footage or images should require the administrative approval of senior personnel.
 - i) Example: The police academy wishes to use crowd shots in training as background footage, or to illustrate some point relating to law enforcement technique, such as conducting an arrest. Whether such secondary uses would be permissible is a decision that should be reserved to accountable, senior decision-makers.
- (3) Release of footage or images should only occur upon written request through a designated chain of command, acting in accordance with relevant privacy laws.
- (4) Operators should not be able to make copies of footage or images without supervisor authorization.
- (5) Private-sector footage or images should be treated as if they had been recorded initially on a government-run camera once they come into government hands. For privacy and data integrity purposes, the footage or images should be considered government footage or images once they are in government hands.
- (6) There is generally no legal expectation of privacy in things in plain view; but if a yard is fenced off, or window curtains are drawn, and technical surveillance is capable of breaching those privacy measures, probable cause or a warrant may be required.
 - i) Certain “public” areas require special attention from legal counsel since individuals may have an expectation of privacy in those areas - consider changing rooms at a public pool or gym, and restrooms.

Data Quality and Integrity Principle

Each government agency should, to the extent practical, ensure that the camera footage or images are accurate, relevant, timely, and complete, within the context of its use.

- (1) Safeguard and authenticate the stored camera data using appropriate physical, personnel, and technical security measures. Consider using digital watermarks, encryption, or other security and authentication techniques to secure the data.
- (2) Consider how the system design may be used to authenticate and establish chain-of-custody for data that will potentially be used as evidence.
- (3) Establish a data retention policy that requires the purging of recorded footage or images that lack evidentiary value or other value for a stated purpose of the system.
- (4) Provide for procedures (a) to identify and secure data that should be retained as evidence or for other stated purposes; (b) to conduct for regularly scheduled review of all retained data; and (c) for the routine destruction/purging of data that does not have to be retained.
- (5) Determine ahead of time how requests for stored data potentially related to third-party litigation will be handled. While agencies must comply with specific subpoena and court orders, there is no objection to having a data storage policy that routinely eliminates stored data after its operational (law enforcement or security) usefulness has ended.

Security Principle

Each government agency should protect the CCTV system through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

- (1) Security measures should be layered. The agency should not rely on one particular security measure to safeguard data but should employ several measures that functionally overlap to ensure the security of data and the overall CCTV system.
- (2) Network security is critical, particularly for wireless systems.
- (3) Other security measures include: physical security of the network and of any viewing and data storage centers; personnel security ensuring those who have access to the system are appropriately vetted; and other security measures as appropriate.
- (4) Implement information security practices and safeguards to enforce all privacy policies. Use technology, such as encryption and access controls, to ensure that the system is only used as authorized and that the camera footage and images are protected against unauthorized use.
- (5) Ensure that those who have access to the system are appropriately trained to maintain the data. Training should be provided for all levels of system operations, from technical personnel to administrator and oversight personnel.
 - a) Training should address Constitutional issues, case law, search and seizure regulations, state and local legislation, ethical considerations, and departmental policy.
 - b) Training should occur prior to assignment to operate a CCTV system and include refresher training at least yearly to reinforce the importance of acceptable behavior.
 - c) The importance of proper training and regular refresher training should be highlighted when potential liability issues are considered. Liability may arise under state privacy or tort law if information is mishandled or misused, and prosecutions and security efforts may be undermined by data corruption or mishandling.
- (6) Oversight of system operators to ensure compliance with policies and good practices may act as another layer of security and may serve to improve system function and reduce potential agency liability, even as it ensures the integrity and utility of the CCTV system.

Accountability and Auditing Principle

Each government agency should be accountable for complying with these principles, providing training to all employees and contractors who use the CCTV system, and auditing the actual use of the CCTV system to demonstrate compliance with these principles and all applicable privacy protection requirements.

- (1) Provide adequate supervision at all times when the CCTV system is operational to reduce the risk of misuse or abuse.
- (2) Establish a control log that documents the names and hours of personnel working each shift; names, times and purpose of entry into the CCTV center by non-assigned personnel; all requests for footage or images; and any noteworthy incidents. To some extent this may be done in automated fashion by the measures suggested in item 3, below.
- (3) Use automated operator logon, access control, and other standard audit features to ensure a clear audit trail is maintained. This enables tracking of abusive use of CCTV assets back to the individual who violated a policy.
- (4) Implement appropriate encryption, watermarking, and other chain-of-custody processes to ensure that camera footage and images are appropriately handled.
- (5) Conduct periodic audits of the system to ensure that all policies are adhered to. Preferably, professional boards or outside government agencies should conduct independent audits.

- (6) Provide sanctions against misuse and abuse of CCTV systems, as well as remedies for people who may be harmed by those types of abuse and misuse. Create technological and administrative safeguards, such as digital masking of people whose images are incidentally captured, but who are not the actual criminal suspects.
- (7) Define consequences for misuse or abuses of the system as part of the written policy and ensure that all users receive training regarding these consequences.
- (8) A useful oversight measure, and one that can help build community trust in the law enforcement agency and in the CCTV system, is to permit public inspection of the CCTV operations center/viewing room at any reasonably appropriate (*e.g.*, non-crisis) time.